IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) In an IEEE 802.11(b) wireless LAN, a method for accessing and analyzing the contents of data packets or frames transmitted along a IEEE 802.11 (b) wireless communication channel, comprising the steps of:

establishing a direct wireless logical connection with the wireless communications network;

receiving wirelessly, in real-time, data packets or frames transmitted in the wireless communications network for all stations or devices associated therewith;

performing over a first period of time a detailed protocol analysis on the contents of the header of the data packets or frames, including analyzing associated protocol layers in detail, permitting a user to enter the MAC addresses of known access points operating in said IEEE 802.11(b) wireless communication channel; selectively activating a rogue access point detection routine; checking the addresses of newly detected access points against the addresses of said known access points; and marking for display as a rogue access point, any access point detected that is not included as a known access point; and

displaying in real time the results of the analysis to a user.

2. (Original) The method of Claim 1, further including the steps of:

storing in a memory storage device, the data packets or frames captured over a second period of time; and

performing an offline detailed analysis on the contents of the IEEE 802.11(b) header of the data packets or frames, and associated protocol layers, stored in the memory storage device; and

displaying the results to the user.

3. (Original) The method of Claim 1, further including the step of:

selectively turning said detailed protocol analysis on or off for a particular protocol layer, whereby for a protocol layer turned off, that layer and all protocol layers above or higher than that layer are not subjected to a detailed protocol analysis.

4. (Original) The method of Claim 1, wherein the step of performing a detailed protocol analysis includes the step of generating alarms for display relating to detected network and protocol errors.

5. (Original) The method of Claim 4, wherein the step of performing a detailed protocol analysis further includes selectively turning on or off said alarm generating step.

6. (Original) The method of Claim 4, wherein the step of performing a detailed protocol analysis further includes the steps of:

assigning a default severity level from a plurality of available severity levels for each available alarm; and

selectively determining whether a particular alarm type is to be logged when generated.

7. (Original) The method of Claim 6, further including the step of selectively marking an alarm as a diagnosis or a symptom dependent upon the detected severity level.

8. (Original) The method of Claim 1, wherein said step of displaying includes the step of showing all layers of protocols analyzed for each capture of frame or data packets.

9. (Original) The method of Claim 8, wherein said step of displaying further includes the step of:

showing the total number of frames and octets analyzed for a selected protocol layer.

10. (Original) The method of Claim 8, wherein said step of displaying includes the step of showing for a selected protocol layer, lower layer objects linked to a current selected object.

11. (Original) The method of Claim 8, wherein said step of displaying includes the step of showing the hosts created for said IEEE 802.11(b) wireless communication layer, and the attributes of said hosts, respectively.

12. (Original) The method of Claim 11, further including showing detailed statistics for each selected host.

13. (Original) The method of Claim 11 further including showing attributes for each selected host including MAC address, station function, frame types, channel, network types, BSSID, and SSID.

14. (Original) The method of Claim 11, further including showing the higher layer DLC objects linked to selected wireless layer hosts, respectively.

15. (Original) The method of Claim 11, further including showing alarms associated with a selected host.

16. (Cancelled)

17. (Currently Amended) A wireless network troubleshooting tool for monitoring an IEEE 802.11(b) LAN wireless communication network to detect and diagnose failures in said wireless communication network, said tool comprising:

a wireless network interface device operable in a promiscuous mode within a wireless communications network for capturing a plurality of frames or data packets transmitted through the network for all stations or devices associated therewith;

a user interface system including input and output devices for enabling a user to input and obtain information associated with said plurality of captured frames;

a memory storage device for storing said plurality of captured frames as received from said wireless network interface device; and

a programmable processor unit connected to said wireless network interface device, said user interface system, and said memory storage device, said processor being programmed to execute a routine comprising the steps of:

establishing a direct wireless logical connection with said wireless communications network via the network interface device;

receiving wirelessly, in real-time, frames transmitted in the wireless communications network via direct wireless logical connection;

receiving from said user, via said user interface, configuration parameters;

performing, through use of said configuration parameters a detailed protocol analysis on the contents of respective headers of the captured data packets or frames, including associated protocol layers, respectively; and

displaying the results of the analysis to the user in real-time;

wherein the detailed protocol analysis includes permitting a user to enter the MAC addresses of known access points operating in said IEEE 802.11(b) wireless communication channel; selectively activating a rogue access point detection routine; checking the addresses of newly detected access points against the addresses of said known access points; and marking for display as a rogue access point, any access point detected that is not included as a known access point.

18. (New) The method of Claim 1, wherein said step of displaying includes utilizing a plurality of viewing panes.

19. (New) The method of Claim 6, wherein, for each available alarm, a user is capable of assigning a severity level chosen from the plurality of available security levels that is different from the default security level.